## REMARKS

Claims 1-79 now stand in the application, new claims 77-79 having been added and various editorial amendments made to the remaining claims. Reconsideration of the application and allowance of all claims are respectfully requested.

The claims have been reviewed and editorially amended. Regarding the issue rasied in paragraph 4 of the Office action, the "for each of" language is believed appropriate and clear in that the step flowing that clause is performed in each of a plurality of tables. The present language is believed the clearest way to describe this. Nonetheless, in some circumstances in the claim it has been amended in an effort at better readability and further clarity.

With respect to paragraph 5 of the Office action, "permutation" is a specific case of "reordering," so the more specific term has been deleted.

With respect to paragraphs 6-8 of the Office action, the issues raised have been addressed by the above amendments.

The present invention as defined in claim 1 is an improvement in implementing the Kasumi algorithm wherein a first set of bits defining the input is used to select an element from each of a plurality of lookup tables, and then a second set of bits from the input is used to select amongst the outputs of the various lookup tables.

The examiner has not identified look-up tables in Kim, nor has the examiner identified which of the bits of the input are considered to be the claimed first set of bits and which are considered to be the claimed second set of bits. But it is in any event clear that in the operation of Kim there is no point at which the first set is used for some process and the second set is used to select from the result of processing the first set.

The examiner cites to lines 13-31 of page 9 of Kim as teaching this feature, but it does not. Lines 13-18 describe the processing of the first set of bits by the first pipeline section 310 to produce a output data, and then Exclusive ORing the output data with the second set of 16 bits of the input to thereby generate an output of the first pipeline section. But this Exclusive OR operation is not the selection of one of the output data bits as is required in claim 1. Symmetrical operations are performed in the subsequent pipeline sections. But it is important to note that the adders 307 at the output of each of the pipeline sections does not select "a corresponding output from the set of outputs" as is required in claim 1.

The '319 patent teaches a block cipher method, but does not make up for this deficiency in Kim. Thus, even if the teachings of the references were combined in some obvious manner, there would be no selection of one of the outputs from the processing of the first set of input bits, as is required in independent claims 1, 12 and 49

For the above reasons, it is submitted that all of claims 1-20 and 49 patentably distinguish over the applied art.

With respect to claim 21, note that the claim requires that there be plural inputs each of plural bits, and a selection of a subset of the input bits. This requires multiple subsets selected from multiple parallel inputs. The examiner cites to page 9 of Kim, but has not identified what is considered to be the claims plurality of inputs. There is one 32-bit input in Fig. 4 of Kim. There is a selection of a subset of the input, but this selection of a subset of the input is not performed for multiple inputs in parallel. That would require replicating Fig. 4 of Kim to have multiple pipeline sequences, but this is not suggested in Kim.

This same feature and distinction over the art are characteristic of claims 35 and 50, so that all of claims 21-48 and 50 patentably distinguish over the applied art.

As to claim 51, the examiner simply reads the claim language and broadly refers to page 9 of Kim, but the subject matter of claim 51 is not found there. Claim 51 requires that that plural inputs each made up of plural bits. Bit re-ordering is performed on the plural-bit inputs to obtain M parallel sets of outputs. The examiner has not identified where the plural bit inputs are, or where the bit re-ordering takes place. The examiner has further not identified where the ith set of those outputs is, or how it defines a respective subset of the input bits. This is simply not taught in Kim, or in any of the secondary art, and allowance of claims 51 -54 is believed in order.

As to claim 55, that claim defines a ciphering method in which there are a plurality of ciphering algorithm inputs, a plurality of first inputs each associated with one of the ciphering algorithm inputs, and each first input is used to address a lookup table. The examiner refers to page 9 of Kim, but provides no explanation other than that "simultaneously is interpreted to be equivalent to in parallel." But the claimed subject matter is simply not taught. Claim 55 requires that there be plural lookup tables each addressed by a respective first input, with all of this done in parallel. Even if look-up tables were used in Kim, the examiner has not shown where this would occur in one function in one of plural enciphering rounds, or how the "first inputs" in this round relate back to the enciphering algorithm inputs. Claim 64 includes similar subject matter, so that it is believed that all of claims 55-73 patentably distinguish over the applied art.

As to claims 74-76, these claims require that a plurality of inputs each be used to address respective lookup tables to provide respective outputs. Bt it is noted that in Fig. 4 of Kim et al, the output of the first stage 310 is only obtained by Exclusive ORing the processed result of the first 16 bits with the second 16 bits, and this is similarly true of each of the stages 320 and 330. Even if look-up tables were to be used in the Kim et al system, the examiner has not explained how, absent the teaching of the present application, the lookup tables would be substituted in just the right way to achieve what is recited in claims 74-76, as opposed to using lookup tables in such a manner that they would not provide the required outputs.

Claims 77-79 have been added to add to claims 74-76 a further distinctive feature of the use of the look-up tables according to the present invention, reflected in certain of the other claims.

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,

/DJCushing/
David J. Cushing
Registration No. 28,703

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Date: January 11, 2008